Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2000*.

2a)☐ This action is **FINAL**.　　2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

　　　　application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date *4*.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-46 have been examined.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   Claims 1-4 and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated

by England et al. (hereinafter refereed to as England) (U.S. Patent No. 6,330,670 B1).

4.   As per claims 1 and 24, England teaches a method for enabling the rendering of

digital content on a device, the method comprising:

transferring the content to the device (column 19, lines 54-61);

obtaining a digital license corresponding to the content (column 10, lines 14-18,

column 19, lines 10-16 and lines 45-53);

composing a sub-license corresponding to and based on the obtained license

and transferring the composed sub-license to the device, to enable rendering of the

content on the device only in accordance with the terms of the sub-license on the device

(column 19 lines 54-67 and column 20 lines 1-7).

5.   As per claims 2 and 25, England teaches the method as applied to claims 1 and

24 above. Furthermore, England teaches the method further comprising, prior to

composing the sub-license and transferring the composed sub-license to the device,

checking the obtained license to determine that such license permits issuance of

the sub-license to the device (column 19, lines 54-58 and column 20, lines 17-19).

6.   As per claims 3, 4, 26 and 27, England teaches the method as applied to claims

1 and 24 above. Furthermore, England teaches the method further comprising:

coupling the device (i.e. other client computers) to a computer (i.e. subscriber

computer) (column 19, lines 54-58);

placing the obtained license on the computer (column 10, lines 14-18, column 19,

lines 10-16 and lines 45-53); and

transferring the composed sub-license from the computer to the device (column

19, lines 65-67 and column 20, lines 1-2).

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 5-10 and 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over England (U.S. Patent No. 6,330,670 B1).

As per claims 5-7 and 28-30, England teaches the method as applied to claims 1 and 24 above. Furthermore, England teaches the method, wherein the content is encrypted and decrypted according to a content key (column 16, lines 53-57), a computer having a public key and a private key corresponding to the public key (column 7, lines 50-61), and authentication of the computer using digital signature of the computer (column 9, lines 60-65). However England does not explicitly teach encrypting the content key using the device's (computer) public key (secret key). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method of encrypting the content key into the authentication and digital signature method thought by England in order to secure the content key.

9.   As per claims 8-10 and 31-33, England teaches the method as applied to claims 5 and 28 above. Furthermore, England teaches the method wherein the composing of the sublicense further comprises placing a rights description, indexing information identifying a secret in the sub-license, the rights description describing rights conferred by the license, the device rendering the corresponding content only in accordance with the rights description (column 19, lines 57-65, fig 9 and fig 11).

10.   Claims 11-13 and 34-36 are rejected under 35 U.S.C 103(a) as being

unpatentable over Downs et al. (hereinafter referred to as Downs) (U.S. Patent No.

6,574,609 B1).

11.   As per claims 11 and 34, Downs teaches A method for rendering digital content

on a device, the method comprising:

        receiving the content onto the device (column 16, line 19), the content being

encrypted and decryptable according to a content key (column 15, lines 55-57);

        receiving a digital license corresponding to the content onto the device (column

18, lines 51-53), the license including the content key encrypted and decryptable

according to a secret (public key, private key) (column 18, lines 48-51);

        applying the secret to the encrypted content key to decrypt and obtain the

content key (column 16, lines 43-45); and

        applying the obtained content key to the encrypted content to decrypt and obtain

the content (column 16, lines 45-47).

        Furthermore, Downs teaches creating a text file containing information about

parts that are included in a package (i.e. licence) (column 38, lines 42), the information

including key description part (i.e. secret public/private keys) (column 40, lines 19-28),

Downs also teaches creating an offer package and store the package in a database

indexed with product ID (column 71, lines 50-53). However Downs doesn't explicitly

teach a license including indexing information identifying a secret to a device. It would

have been obvious to one having ordinary skill in the art at the time the invention was

made to implement a license having indexing information identifying a secret into the

text file containing secret information thought by Downs, so that the text file of Downs

can be implemented as an indexed database as per teachings of Downs (column 71,

lines 50-53).

12.   As per claims 12 and 35, Downs teaches the method as applied to claim 11 and

34 above. Furthermore, Downs teaches the method, wherein the license includes a

signature, the method further comprising verifying the license based on the signature

thereof and the secret (column 16, lines 19-25).

13.   As per claims 13 and 36, Downs teaches the method as applied to claim 11 and

34 above. Furthermore, Downs teaches the method, wherein the license includes a

rights description describing rights conferred by the license, the method comprising

rendering the corresponding content only in accordance with the rights description

(column 19, lines 9-37).

14.   Claims 14-23, and 37-46 are rejected under 35 U.S.C 103(a) as being

unpatentable over Matias et al. (hereinafter refereed to as Matias).

15.   As per claims 14, 19, 37 and 42, Matias teaches a method for composing a

license for rendering digital content on a device, the content being encrypted and

decryptable according to a content key, the device having an identifier, the method

comprising:

deriving (generating) a secret (i.e. a shared key) (column 2, lines 5-10) by:

obtaining the device identifier (client identifier) (column 2, line 7) ;

acquiring a super-secret (i.e. secret client information) that is also acquirable by

the device (column 2, line 8); and

applying the obtained device identifier and super-secret to a function to derive

the secret (column 2, lines 5-10):

(SECRET) (i.e. shared key) = function (device identifier, (SUPER-SECRET))

(column 5, lines 65-67 and column 6, lines 1-8);

Furthermore, Matias teaches encrypting / decrypting data using the generated

shared key (column 6, lines 25-34). However Matias does not explicitly teach using the

generated key to encrypt a content key and placing the content key in the license. It

would have been obvious to one having ordinary skill in the art at the time the invention

was made to encrypt the content key and store it in the license into the method of using

a generated secret key to encrypt data thought by Matias, so that the encrypted content

key can be the encrypted content data as per teachings of Matias.

16.   As per claims 15, 19, 38 and 43 Matias teaches the method as applied to claims

14, 19, 37 and 42 above. Furthermore Matias teaches the method, wherein the content

has a content ID, the method comprising deriving a secret by:

obtaining the content ID (server ID) of the content (column 4, line 12);

obtaining the device identifier (client ID) (column 4, line 12);

acquiring a super-secret (secret information) that is also acquirable by the device

(column 4, line 14); and

applying the obtained content ID, device identifier, and super-secret to a function

to derive the secret (column 4, lines 9-15):

(SECRET) (i.e. shared key)= function (content ID, device identifier, (SUPER-

SECRET)) (column 5, lines 65-67 and column 6, lines 1-8).

17.   As per claims 16-18, 20-22, 39-41 and 44-46 Matias teaches the method as

applied to claims 14, 19, 37 and 42 above. Matias teaches driving a secret key (shared

key) according to a function of device identifier (client identifier), content identifier

(server identifier) and super-secret information (column 4, lines 7-15), and encrypting /

decrypting data using the derived secret key (shared key) (column 6, lines 25-34). But

identifying the secret key by indexing information is not explicitly mentioned. However,

Official notice is taken that it is well known to store data and index information to identify

stored data in order to identify stored data and make searching data efficient.

Conclusion

18.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

a)   U.S. Patent No. 6,233,567 B1 discloses a method and apparatus for software licensing electronically distributed programs.

b)   U.S. Publication No. 2001/0052077 A1 discloses a universal mobile ID system and method for digital rights management.

c)   U.S. Publication No. 2001/0056539 A1 discloses a software protection device and method.

d)   U.S. Patent No. 5,953,420 to Matyas Jr. et al. discloses a method and apparatus for establishing an authenticated shared secret value between a pair of users.

e)   U.S. Patent No 6,094,487 to Butler et al. discloses an apparatus and method for encryption key generation.

f)   U.S. Publication 2003/0194094 A1 to Lampson et al. discloses a system and method for secure storage data using a key.
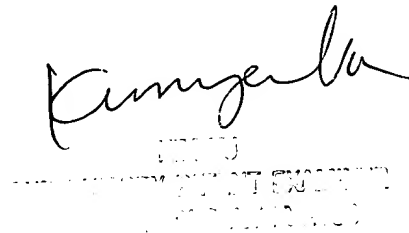

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

March 18, 2004